Juniper Networks

SNMP Monitoring Guide

Applicable for:
Secure Access Service
MAG Series Junos Pulse Gateway
Access Control Service

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
408-745-2000
www.juniper.net

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Juniper Networks SNMP Monitoring Guide

Table of Contents

OVERVIEW

This document describes guidelines for SNMP monitoring of Secure Access devices' health and stability. The MIB OIDs and functions in the tables provided are from the Juniper Networks MIB and UC Davis MIB.

Most objects explained in this document are also included in the Juniper SA/MAG/IC Software Administration Guide. The Juniper Networks MIB has all the necessary objects that can be used for monitoring most of the components while the UCD MIBs has a few useful objects and is added for information. Standard SNMPv2 MIB is also supported but not included in this document.

PROCEDURE

1. Download the Juniper Networks MIB from the device Admin UI SNMP page. This has most of the objects for MAG/SA SNMP monitoring (See NOTES below).

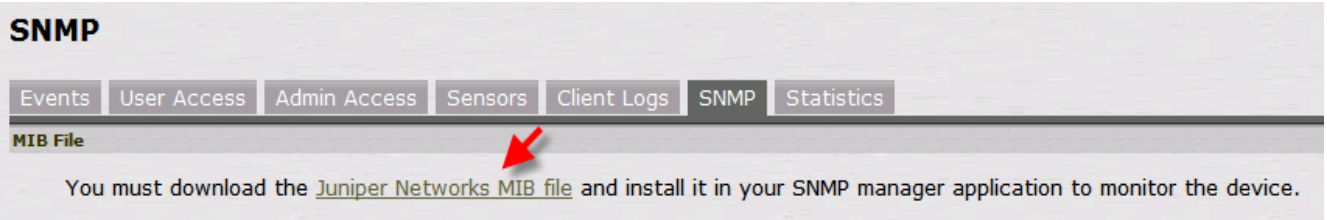
2. To monitor system statistics, such as memory utilization, load the UC-Davis MIB file into the SNMP manager application. You can obtain the MIB file from:

   http://net-snmp.sourceforge.net/docs/mibs/UCD-SNMP-MIB.txt

3. Install the MIBS to monitor your device and use the OIDs described in the tables shown later in this document.

NOTES

- SMMPv2 standard MIB and the UCDavis MIB are supported, but most of the needed objects for monitoring stabiity are already available through the Juniper Networks MIB downloadable from the Admin UI SNMP page.



- Safe and critical values are essentially guides to assist in establishing some monitoring. Adjustments may be necessary depending on configurations to be done on the devices but most of the values are known best practice values and recommendations.

COMMON OBJECTS FOR SNMP MONITORING OF MAG/SA DEVICES

Below are most of the objects that can be used for monitoring the health of an SA or MAG system.

NOTE: A full list of objects can be found in the 7.3 admin guide (pages 903-907) located at http://www.juniper.net/techpubs/software/ive/admin/j-sa-sslvpn-7.3-adminguide.pdf

JUNIPER MIB:

COMPONENT	OID	DESCRIPTION	TRAP	POLL	MORE INFORMATION
USERS	.1.3.6.1.4.1.12532.2.0	Number of signed-in web users		Y	Monitors users connected and uses the web feature. Not critical in monitoring health: informational only.
	.1.3.6.1.4.1.12532.12.0	Total number of users logged in to the SA node		Y	Monitors the number of users in this node that are logged in. Not critical in monitoring health: informational only.
	1.3.6.1.4.1.12532.13.0	Total number of users logged in to the Cluster		Y	Monitors the number of users in the cluster that are logged in. This number counts towards the user licenses. Not critical in monitoring health: informational only.
	.1.3.6.1.4.1.12532.251.6	Maximum number of concurrent users signed in	Y		Traps based on Admin UI settings (see Figure 1). Setting determined by the administrator. Critical trap to inform that the user license limit is reached.
	.1.3.6.1.4.1.12532.9.0	The number of concurrent meeting users	Y		Monitors the number of secure meeting users connected. This number counts towards Secure Meeting license, cannot be queried and accessed for notification only via trap. Not critical in monitoring health: informational.

	.1.3.6.1.4.1.12532.251.17	Concurrent meeting count over license limit	Y		Traps based on Admin UI settings (see Figure 1). Setting determined by the administrator. Critical trap to inform that the user license limit is reached.
MEMORY	.1.3.6.1.4.1.12532.11.0	The Memory Utilization of the IVE system		Y	Depending on the load and features used: <90% is normal 90-95% is high but not necessarily an issue ACTION: Start monitoring swap 95-99% is very high but not necessarily will cause immediate issue ACTION: Start monitoring swap
	.1.3.6.1.4.1.12532.251.21	IVE memory utilization above threshold	Y		Traps based on Admin UI settings (see Figure 1) See also above for safe usage. ACTIONS: Set the Memory trap setting in UI to very high (95% to 99% as Linux systems can use most of physical memory and does not fully indicate issues. Start monitoring swap for usage when trap starts to be generated. **SEE NOTES
	.1.3.6.1.4.1.12532.24.0	The Swap Utilization of the IVE system		Y	0% is normally what swap usage should be. From 5% of swap usage, it needs monitoring ACTION: If swap starts to be

					utilized, get logs. **SEE NOTES
	.1.3.6.1.4.1.12532.251.23	IVE swap utilization above threshold	Y		Same as above ACTION: Recommended to set to 5%. When trapping starts, get logs. **SEE NOTES
CPU	.1.3.6.1.4.1.12532.10.0	The CPU Utilization of the IVE system		Y	Depending on the load and features used: <50% is usually normal Above or steady at 80%, especially during peak times, may indicate load issue. 100% is abnormal and needs investigation Sudden jump leading to 100% is not normal when it does not come down within few minutes. CPU of 100% steady is not normal. ACTION: Check usage, throughputs from graphs and re-evaluate capacity. Get logs. **SEE NOTES
	.1.3.6.1.4.1.12532.251.22	IVE CPU utilization above threshold	Y		Traps based on Admin UI settings (see screeshot*) See above for CPU values. It is recommended to not set CPU trap until the normal CPU usage is known. ACTION: If it is known, set CPU trap to default of 80% in admin SNMP page. If it traps at 80% consistently, get logs. See Figure 1 and “NOTES

					ON LOGS" later in this document.
DISK	.1.3.6.1.4.1.12532.25.0	Percentage of disk space		Y	<80% is normal 80% and above needs close monitoring 90% and above is critical ACTION: If disk space percentage starts to go over 80%, gather logs See "NOTES ON LOGS" later in this document.
	.1.3.6.1.4.1.12532.251.18	Disk space nearly full	Y		Traps based on Admin UI settings (see Figure 1) ACTION: Recommended to set to 90%. If it continously traps, start monitoring and gathering logs. See "NOTES ON LOGS" later in this document. Backup and delete logs immediately, delete all snapshots if seen. Clear out debuglogs if set to high value, call Juniper Support for assistance.
	.1.3.6.1.4.1.12532.251.19	Disk space full	Y		Disk usage has gone 100%. This is a critical isue as this will eventually crash box. ACTION: Backup and delete logs immediately, delete all snapshots if seen. Clear out debuglogs if set to high value, call Juniper Support for assistance. Getting more logs may not work due to space exhausted.
LOG	.1.3.6.1.4.1.12532.1.0	Percentage of log file full		Y	This reading can help determine if archiving is

					needed or modified. Not critical in monitoring health: informational.
	.1.3.6.1.4.1.12532.251.4	Log file nearly full	Y		This reading can help determine if archiving is needed or modified. Not critical in monitoring health: informational
	.1.3.6.1.4.1.12532.251.5	Log file full	Y		Log file has reached 100% and full. Inidication that log settings may need to be reviewed or archiving settings needed to be modified. Not critical in monitoring health: informational only.
TEMPERATURE	.1.3.6.1.4.1.12532.42.0	The Temperature of MAG application blade		Y	This is a critical information for stability of the chassis/blades < 75 deg C is normal From 70 deg C, monitor temperature closely as a precaution 75 deg C and above is not normal and will fire a trap ACTION: Check admin UI temperature to confirm, check other blades as well, check fans and status of LEDs, get outputs from CMC CLI (if used) commands to get status of each blades and alarms. Call Juniper support.
	.1.3.6.1.4.1.12532.251.35	IVE Temperature is above threshold	Y		This is a critical trap Traps at 75 deg C ACTION: Check admin UI temperature to confirm,

					check other blades as well, check fans and status of LEDs, get outputs from CMC CLI (if used) commands to get status of each blades and alarms. Call Juniper support.
POWER SUPPLIES	.1.3.6.1.4.1.12532.251.27	The status of the power supplies has changed	Y		This is a critical trap to know fan status, which is any of the following: "Both the power supplies are back up" "One of the power supplies has failed" ACTION: Investigate further and call Juniper support.
FANS	.1.3.6.1.4.1.12532.251.26	The status of the fans has changed	Y		This is a critical trap to know fan status, which is any of the following: “Fan N is running above threshold (xyz RPM)” “Fan N is running below threshold (xyz RPM)” "Both the fans are back up" "Both the fans have failed" "One of the fans has failed" ACTION: Investigate further and call Juniper support.
HARD DRIVES	.1.3.6.1.4.1.12532.251.28	The status of the RAID has changed	Y		This is a critical trap to know RAID status, which is any of the following: "The RAID status is OK" "The RAID status is recovering" "The RAID status is unknown"

					"The RAID status is failed" ACTION: Investigate further and call Juniper support.
NETWORK INTERFACES	.1.3.6.1.4.1.12532.251.33	The Internal interface has gone down, reason is in nicEvent	Y		This is a critical trap ACTION: Investigate further
	.1.3.6.1.4.1.12532.251.34	The Management interface has gone down, reason is in nicEvent	Y		This is a critical trap ACTION: Investigate further
	.1.3.6.1.4.1.12532.251.31	The External interface has gone down, reason is in nicEvent	Y		This is a critical trap ACTION: Investigate further

UC DAVIS MIB:

COMPONENT	OID	DESCRIPTION	TRAP	POLL	MORE INFORMATION
MEMORY	.1.3.6.1.4.1.2021.4.11.0	Total Available Memory on the host		Y	Compared to Juniper MIB, this reads size in Bytes or Mbytes so it needed to be converted to percentage. Depending on the load and features used (% of total memory of system): <90% is normal 90-95% is high but still fine ACTION: Start monitoring swap 95-99% is very high but not necessarily will cause immediate issue ACTION: Start monitoring swap
	.1.3.6.1.4.1.2021.4.4.0	Available Swap Space on the host.		Y	Compared to Juniper MIB, this reads size in Bytes or Mbytes. Can be computed in

					percentage, like Juniper MIB: From 5% of swap usage, it needs monitoring 0% is normally what swap usage should be. ACTION: If swap starts to be utilized, get logs. See "NOTES ON LOGS" later in this document.

CRITICAL/MAJOR EVENTS

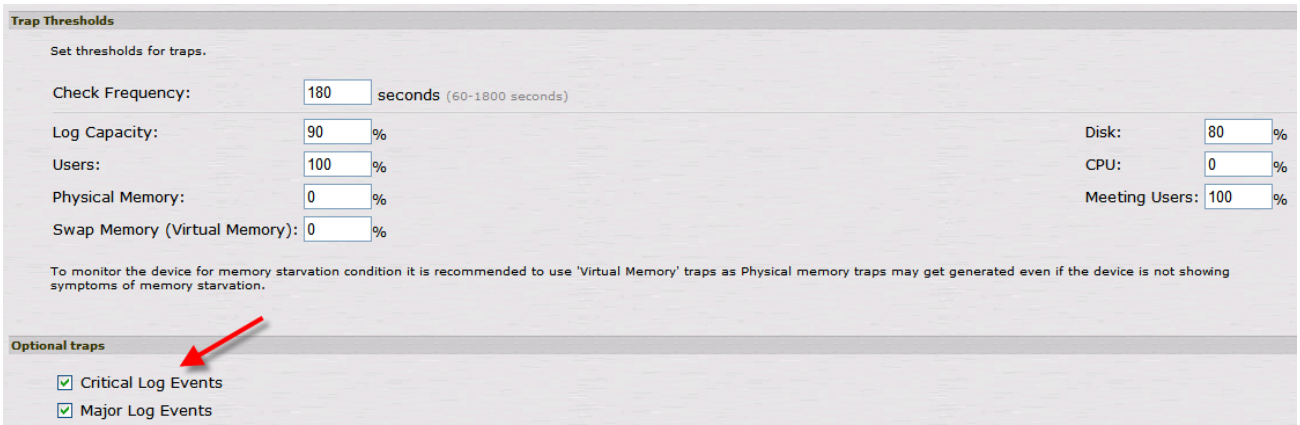
Monitoring "Critical" and "Major" events augments the polling and trapping values obtained from the available OIDs supported in the system. There are log messages that are important to monitor as well, and both "Critical" (Level 10) and "Major" (Level 8-9) are available for use in SNMP monitoring. The list of logs can be obtained from Juniper Networks Technical Support.

Some examples are:

SYS10047	SystemStatus	ClusterMsg	InternalInterfaceDown	10	internal NIC down.
SYS10049	SystemStatus	ClusterMsg	ExternalInterfaceDown	10	external NIC down.
SYS10051	SystemStatus	ClusterMsg	InternalGatewayDown	10	internal gateway '%1' unreachable.
SYS10053	SystemStatus	ClusterMsg	ExternalGatewayDown	10	external gateway '%1' unreachable.
ERR20643	SystemError	Misc	RestartSvc	10	Watchdog restarting services (%1).
ERR30431	SystemError	Misc	RestartProcesses	10	Watchdog restarting %1 processes (%2).

The Critical Log events and Major Log events can be included in SNMP monitoring by checking the options in the SNMP page as shown in Figure 1.

Figure 1: Screenshot of SNMP Options:



NOTES ON LOGS:

Log needed at the minimum from the SA or IC devices or MAG blades:

- System snapshot (**Troubleshooting > System Snapshot > (select to include debuglog and configs) > Take snapshot**)
- SA/MAG logs (**Log/Monitoring > Events logs > Save all logs**)
- Screenshot of the cockpit graph detailing issue time and readings without cropping (showing date information)